

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA**

| | | |
|-------------------|---|--------------------------|
| JOHN FOLINO, |) | |
| |) | |
| Plaintiff, |) | Civil Action No. 17-1584 |
| |) | |
| v. |) | Judge Cathy Bissoon |
| |) | |
| MICHAEL HINES and |) | |
| ALISON LY, |) | |
| |) | |
| Defendant. |) | |

MEMORANDUM AND ORDER

Pending before the Court is the Motion for Sanctions Against Defendant Alison Ly (hereinafter “Sanctions Motion,” Doc. 22) filed by Plaintiff John Folino (“Folino” or “Plaintiff”) and the Response in Opposition (hereinafter “Response,” Doc. 26) of Defendant Alison Ly (“Defendant Ly”). For the reasons that follow, Plaintiff’s Sanctions Motion will be **GRANTED**.

I. MEMORANDUM

A. BACKGROUND

Plaintiff initiated this suit under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, against 13 John Doe Defendants in December of 2017, after his personal e-mail account was accessed without his permission. (Plaintiff’s Complaint at ¶¶ 15, 28, Doc. 1.) After the Court granted Plaintiff’s Motion for Expedited Discovery (Doc. 5) to uncover the personal identifying information of the John Doe Defendants, on February 6, 2018, Plaintiff filed an Amended Complaint against the named Defendants, Michael Hines and Alison Ly. (Plaintiff’s Amended Complaint, hereinafter “Amended Complaint,” Doc. 6). Plaintiff seeks damages caused by the unauthorized access to his e-mail. (*Id.* at ¶ 35.)

Defendant Ly was afforded additional time—until April 6, 2018—to respond to the Amended Complaint, but she did not do so. (Doc. 12.) The Court held a telephone conference on September 18, 2018 (Doc. 19), during which counsel for Defendant Ly and Plaintiff¹ explained that those parties had executed a Settlement and Tolling Agreement (hereinafter, “Settlement Agreement,” Doc. 23-2). The terms and effect of the Settlement Agreement were contested, and the Court invited the parties to file any motions necessary to resolve those issues by October 15, 2018. (Doc. 20.) On that date, Plaintiff filed his Sanctions Motion. (Doc. 22.)

In the Sanctions Motion, Plaintiff states that shortly after the Amended Complaint was served on Defendant Ly, her attorney stated she “had no involvement in or knowledge of any hacking of Mr. Folino’s computers.” (Id. at ¶ 7.) In light of these representations and the prevalence of remote hacking through a third-party computer, Plaintiff agreed to settle the case against Defendant Ly in exchange for the ability to examine her computers to gather evidence and confirm her representations. (Id. at ¶¶ 8–9.) The Settlement Agreement formalizing these terms was executed by Defendant Ly and Plaintiff on April 27, 2018. (Id. at ¶ 14.)

Plaintiff retained an expert to conduct the examination of Defendant Ly’s computers (Id. at ¶ 15; Expert Report of Jason Brannon, hereinafter “Forensic Examination Report,” Doc. 23-3.). Three devices—two iPads and a laptop computer (the “Devices”)—were examined on July 9, 2018. (Affidavit of Lucy E. Hill, Esq., hereinafter “Hill Aff.” at ¶ 12, Doc. 23.) The Forensic Examination Report revealed that on April 26, 2018, the two iPads were both wiped of all data when a factory reset was performed. (Forensic Examination Report at 4). The computer had also been wiped of all active data. (Id.) The forensic examination team determined that it is not

¹ Defendant Michael Hines filed his Answer to the Amended Complaint on April 24, 2018. (Doc. 16.) As such, while his counsel was aware of the status conference, counsel elected not to attend.

possible to recover the data on any of the Devices. (Doc. 23-4 at 1.) Without the data, Plaintiff contends it is not possible to verify Defendant Ly’s claims that she was not involved in the hacking, to trace any potential third-party hacker, or to determine whether the hacking is related to other litigation involving Plaintiff. (Sanctions Motion at 19.)

On August 20, 2018, after receiving the Forensic Examination Report, Plaintiff’s counsel sent a letter to Defendant Ly’s counsel demanding an explanation for the lack of data on her Devices. (Doc. 23-5 at 1.) Plaintiff’s letter stated that unless a truthful explanation was provided, sanctions would be pursued. (Id. at 2.) Plaintiff avers that no explanation has been given. (Hill Aff. at ¶ 22.)

In her Response, Defendant Ly denied hacking Plaintiff’s computer and stated any connection of her IP address with any hacking “is a result of fraud, deceit, and artifice by third parties or erroneous information.” (Response at ¶ 5.) Defendant Ly also denied wiping the hard drive, resetting the iPads, or committing any spoliation of evidence. (E.g., id. at ¶¶ 16, 17, 20.) Plaintiff admitted that the Devices were in her home but avers that she lacks the ability to destroy the data on them. (Id. at ¶ 21.)

B. ANALYSIS

In his Sanctions Motion, Plaintiff seeks default judgment and imposition of costs and fees against Defendant Ly for spoliation of evidence. (Sanctions Motion at ¶¶ 30–43.) Because the evidence at issue is electronically stored information, Federal Rule of Civil Procedure (“Rule”) 37(e) provides the framework for considering whether sanctions are appropriate.² The Rule states:

² The Court, of course, also has inherent authority to sanction, but finds that in this case Rule 37 provides the strongest basis for the sanctions imposed. See Clientron Corp. v. Devon IT, Inc.,

“If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:

(1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or

(2) only upon finding that the party acted with the intent to deprive another party of the information’s use in the litigation may:

(a) presume the lost information was unfavorable to the party;
(b) instruct the jury that it may or must presume the information was unfavorable to the party; or
(c) dismiss the action or enter a default judgment.”

See also Bull v. United Parcel Service, Inc., 665 F.3d 68, 73–74 (3d Cir. 2012) (“Spoliation occurs where: the evidence was in the party’s control; the evidence is relevant to the claims or defenses in the case; there has been actual suppression or withholding of evidence; and, the duty to preserve was reasonably foreseeable to the party.”). The decision of whether to impose sanctions is within the sound discretion of this Court. McLaughlin v. Phelan Hallinan & Schmieg, LLP, 756 F.3d 240, 248–49 (3d Cir. 2014); Bull, 665 F.3d at 72–73 (“Sanctions for spoliation of evidence are reviewed for an abuse of discretion.”).

The factual findings necessary to warrant action by the Court are made easily. First, the lost data on the Devices “should have been preserved in the anticipation or conduct of litigation.” On March 27, 2018, Defendant Ly, through her attorney, accepted Plaintiff’s offer to negotiate a settlement “if Defendant Alison Ly cooperates with a forensic investigation of all computers (including tablets, iPads, etc.).” (Doc. 23-1 at 2.) The iPads were wiped of all data on April 26, the day prior to Defendant Ly’s execution of the Settlement Agreement, in which she agreed to

894 F.3d 568, 577 n.4 (3d Cir. 2018) (stating the preferred course is for district courts to use statutory or rule-based sanctions where they are adequate).

examination of the Devices to verifying her denials that “she or any person in her household” intentionally accessed Plaintiff’s computer. (Settlement Agreement at 1–2.) Access to the lost data was the most important information to Plaintiff in this litigation, and his offer to settle was “contingent” on obtaining it. (Doc. 23-1 at 4.) Second, Plaintiff’s forensic expert determined that the information could not be recovered from the Devices. (Doc. 23-4 at 2.) There is no other source of the information.

Next, the Court must determine whether Defendant Ly acted with “intent to deprive” Plaintiff of the information on the Devices. When electronically stored evidence is lost, but a plausible, good faith explanation is given as to how the evidence became unavailable, Rule 37(e)(1) sanctions are appropriate. E.g., Sinclair v. Cambria Cty., No. 17-149, 2018 WL 468911, at *2–3 (W.D. Pa. Sept. 28, 2018) (awarding sanctions of costs and fees under Rule 37(e)(1) where relevant text messages were allegedly deleted automatically and by mistake). If, on the other hand, a party acts in bad faith with intent to conceal the evidence from its opponent, the harshest sanctions under Rule 37(e)(2) are available. E.g., Goldrich v. City of Jersey City, No. 15-885, 2018 WL 4489674, at *1–2 (D.N.J. Sept. 19, 2018) (finding intent to deprive and imposing sanctions under Rule 37(e)(2) where plaintiff stated a “virus” made information unavailable, but forensic examination showed he gave opponent a computer with no data that was not even used during the relevant time frame); see also Bull, 665 F.3d at 79 (A “finding of bad faith is pivotal to a spoliation determination.”). A finding of intent to deprive may be based on circumstantial evidence. Goldrich, 2018 WL 4489674, at *2.

The Court concludes that Defendant Ly acted with an intent to deprive Plaintiff of the data on the Devices. The Devices were in Defendant Ly’s possession, only an intentional action

could have reset the iPads and wiped the computer, and the destruction of the data occurred at a point in time where she was acutely aware of its importance to Plaintiff.

First, with respect to possession, in her Response, Defendant Ly “admit[s] the devices were in her home.” (Response at ¶ 21.) Defendant Ly represented that she had the ability and was willing to give the Devices to Plaintiff for a forensic examination. (Settlement Agreement at ¶ 1.) These two facts are sufficient to find that Defendant Ly had control over the Devices and can be held accountable for the spoliation which occurred. See First Sr. Fin. Grp. LLC v. Watchdog, No. 12-1247, 2014 WL 1327584, at *5 (E.D. Pa. Apr. 3, 2014) (finding computer was in custody of party accused of spoliation where it was in the home, she had access to it, and proposed she could image the computer for her opponent).

Second, a factory reset of the iPads and the wiping of the hard drive were performed after Defendant Ly knew how important the evidence on those Devices was to Plaintiff and his lawsuit. This action could not have occurred without intent. Cf. id. at *8 (finding reinstallation of Windows software after wiping clean the previous information “would not occur spontaneously without significant input by a user of the computer”).

Finally, the timing of the destruction of the data on the Devices—at the conclusion of the parties’ negotiation of an offer to settle by Plaintiff contingent on Defendant Ly’s willingness to have a forensic examination performed on those same Devices—evinces bad faith. Cf. Bozic v. City of Washington, 912 F. Supp. 2d 257, 270–71 (W.D. Pa. Dec. 5, 2012) (finding defendant committed spoliation and destroyed audio recording of “central event in the case” in bad faith when defendant knew litigation of issues discussed was likely).

As the Court has determined that Defendant Ly acted with intent to deprive, all the sanctions of Rule 37 are available in this case. When considering which sanctions to impose

under Rule 37(e)(2), the following factors act as a guide: “(1) the degree of fault of the party who altered or destroyed the evidence; (2) the degree of prejudice suffered by the opposing party; and (3) whether there is a lesser sanction that will avoid substantial unfairness to the opposing party and, where the offending party is seriously at fault, will serve to deter such conduct by others in the future.” Schmid v. Milwaukee Elec. Tool Corp., 13 F.3d 76, 79 (3d Cir. 1994). After weighing these factors, it is the Court’s determination that the egregious nature of Defendant Ly’s conduct in this case warrants the harshest sanction available: default judgment in favor of Plaintiff.

First, the Court agrees with Plaintiff that the degree of fault is high. “A strong degree of fault exists where ‘there has been actual suppression or withholding of evidence.’” Gentex Corp. v. Sutter, 827 F. Supp. 2d 384, 391 (M.D. Pa. 2011) (quoting Brewer v. Quaker State Oil Refining Corp., 72 F.3d 326, 334 (3d Cir. 1995)). As discussed above, the Devices were in the control of Defendant Ly, the destruction of data was intentionally performed, and a majority of that destruction occurred in very close proximity to her agreement to settle. The strength of the circumstantial evidence leads the Court to conclude that Defendant Ly knowingly suppressed the information on the Devices.

Second, the prejudice to Plaintiff is also very high. As the 2015 Advisory Committee Notes to Rule 37(e) explained, ‘An evaluation of prejudice from the loss of information necessarily includes an evaluation of the information’s importance in the litigation.’ The evidence destroyed by Defendant Ly was critical: it was the evidence which could determine who hacked Plaintiff’s computer and there is no other evidence that exists which can prove liability for the underlying claim. While it may be more appropriate to sanction a party with a presumption of jury instruction when destroyed evidence is not unique, when the evidence is lost

completely and is central to the case, the harsh sanction of default judgment may be warranted. Compare Roadrunner Transp. Servs., Inc. v. Tarwater, 642 F. App'x 759, 759 (9th Cir. 2016) (finding no abuse of discretion where district court granted default judgment against party that “deleted emails and files from his laptops after multiple preservation demands” that were the “primary evidence” in the case) with Edelson v. Cheung, No. 13-5870, 2017 WL 150241, at *4 (D.N.J. Jan. 12, 2017) (declining to impose default judgment, and instead sanctioning defendant with a jury instruction, where the defendant destroyed e-mails but there was additional evidence in the record which could prove plaintiff’s allegations). Because Plaintiff has shown the evidence cannot be recovered and no other evidence can stand in its place, this factor also favors imposition of default judgment.

Third, the Court does not believe that other sanctions would be sufficient, nor does it believe that a lesser sanction would appropriately deter. In coming to this conclusion, the Court is cognizant that granting default judgment is a last resort, recommended only for those instances that cannot be remedied with a lesser sanction. Baliotis v. McNeil, 870 F. Supp. 1285, 1289 (M.D. Pa. 1994). However, on these facts, it is the Court’s determination that no other sanction is effective or is fair to the Plaintiff. While the Court, too, may have been sympathetic—as Plaintiff was—to Defendant Ly’s assertion that she had no role in the hacking, her destruction of evidence has entirely deprived Plaintiff of the ability to know who was responsible for the illegal access of his computer. This destruction is the equivalent of destruction of Plaintiff’s case and a flouting of the law. See Gentex, 827 F. Supp. 2d at 391 (Granting sanction of default judgment in part because of the “deterrence value of harsh sanctions in cases like this where the crucial evidence exists in electronic form, and a party may destroy its opponent’s case with the mere

click of a button.”). Default judgment is the only sanction that adequately forces Defendant Ly to answer for this conduct.

Finally, the Court’s conclusion that the harshest sanction of default judgment is appropriate is strengthened by the fact that Defendant Ly failed to offer *any explanation at all* of what happened to the data on the Devices. Rather, she continued to repeat categorical denials that she committed any spoliation. (See generally Response.) Plaintiff clearly demanded a truthful explanation of what happened to the data long before the instant Motion was filed, and stated that unless Defendant Ly provided that information, sanctions would be pursued. (See Doc. 23-5 at 1-2.) The absence of any explanation—including of accidental or mistaken destruction—in the face of multiple opportunities to explain convinces the Court that no such good faith explanation exists. Rather, Defendant Ly has destroyed the central evidence in this case in bad faith.

In addition to granting default judgment for Plaintiff, the Court will also award the costs and fees incurred to file the instant motion and for the futile forensic examination of Defendant Ly’s Devices as sanctions. See Bozic, 912 F. Supp. 2d at 274 (awarding monetary sanctions to “properly allocate litigation costs” incurred as a result of destroyed evidence). The total costs and fees incurred for both these undertakings is \$13,858.48, and this full amount is awarded to Plaintiff (Hill Aff. at ¶ 21-23; Doc. 23-6.)

* * *

II. ORDER

Plaintiff's Motion for Sanctions Against Defendant Alison Ly (Doc. 22) is **GRANTED**.

An award of monetary sanctions for costs and fees is entered, in favor of Plaintiff and against Defendant Ly, in the amount of **\$13,858.48**. **DEFAULT JUDGMENT** is entered against Defendant Ly. The Court will hold a hearing on the issue of damages for Plaintiff's underlying claim on January 15, 2019 at 10:30am.

IT IS SO ORDERED.

November 14, 2018

s\Cathy Bissoon

Cathy Bissoon

United States District Judge

cc (via ECF email notification):

All Counsel of Record